REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-8 are currently pending in the present application, Claims 1, 3-5, and 8 having been amended. Support for the amendments to Claims 1 and 5 is found at least in the specification at page 18, lines 2-7. Thus, no new matter is added.

In the outstanding Office Action, Claims 1 and 5 were rejected under 35 U.S.C. §112, second paragraph; and Claims 1-8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shirakawa et al. (U.S. Pat. Pub. No. 2002/0051536, hereinafter "Shirakawa").

In reply, regarding the 35 U.S.C. §112, second paragraph rejection, Claim 1 and 5 have been amended to address the rejection set forth on page 2 of the outstanding Office Action. Specifically, Claims 1 and 5 have been amended to address what happens if the condition on the "if" statement is not met. Thus, the 35 U.S.C. §112, second paragraph rejection is believed to have been overcome.

Regarding the 35 U.S.C. §103 rejection, Claim 1 recites, *inter alia*, a tamper resistant micro- processor that executes a plurality of programs in parallel under a multi-task programming environment, including:

> a cache memory configured to store the execution code or data decrypted by the decryption unit into one of cache lines provided in the cache memory, ***each cache line having a secret protection attribute holding section for storing an actual encryption key*** used in decrypting the execution code or data, the execution code or data stored in the cache memory remaining even after each program terminates; and
>
> the cache memory control unit configured to process a reading request for the execution code or data to be acquired from the decryption unit or the cache memory such that, if the execution code or data exists in the cache memory and the actual encryption key stored in the secret protection attribute holding section of a cache line that stores the existent execution code or data is identical with the prescribed key corresponding

> to a program that issues the reading request, the execution code or data in the cache memory is read out, ***and if the execution code or data does not exist in the cache memory or the actual encryption key is not identical with the prescribed key, the execution code or data is read out from an external memory device.***

Accordingly, in Claim 1 (and similarly in independent Claim 5), each cache line has a secret protection attribute holding section for storing an actual encryption key used in decrypting the execution code or data. Additionally, in Claim 1 (and similarly in independent Claim 5), if the execution code or data does not exist in the cache memory or the actual encryption key is not identical with the prescribed key, the execution code or data is read out from an external memory device.

The outstanding Office Action concedes on page 4 that Shirakawa does not disclose "each cache line containing a holding section for storing the encryption key used in decrypting the execution code or data." Further, the Office Action asserts that "Shirakawa discloses a 'key pair tag' which is used as an index of the key pair table." The Office Action (at page 4) continues to assert that it would have been obvious to "store the key in the cache line as it would save time at the cost of storage as it is directly being read from the cache in instead of being fetched every time." No evidence has been cited to support this conclusion, as the case law requires. Note, for example, In re Gartside, 203 F.3d 1305, 1315, 53 USPQ 1769, 1775 (Fed. Cir. 2000).

Further, Shirakawa does not teach or suggest the possibility that a key in a cache is not identical with the key fetched and read from the key pair table according to the 'key pair tag,' nor what function to perform if this were the case. That is, Shirakawa does not describe the scenario that is to occur when the actual encryption key is different from the prescribed key corresponding to a program that issues a reading request. Therefore, Shirakawa does not teach or suggest that if the execution code or data does not exist in the cache memory or the

actual encryption key is not identical with the prescribed key, the execution code or data is read out from an external memory device, as recited in Claim 1.

Consequently, Shirakawa does not teach or suggest all of the elements in Claim 1. Accordingly, it is respectfully submitted that Shirakawa does not anticipate or make obvious the features of Claim 1. Therefore, Claim 1 is believed to patentably define over Shirakawa for all of the above reasons.

Independent method Claim 5 recites similar features as argued above for independent Claim 1. For substantially the same reasons as discussed with regard to Claim 1, it is respectfully submitted that independent Claim 5 also patentably defines over Shirakawa.

With regard to the rejection of Claims 2-4 and 6-8 as unpatentable over Shirakawa, it is noted that Claims 2-4 and 6-8 are dependent from either Claim 1 or Claim 5, and thus are believed to be patentable for at least the reasons discussed above.

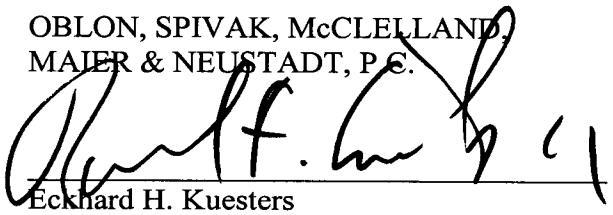
Further regarding the rejection of Claims 2 and 6 as unpatentable over Shirakawa, the Office Action incorrectly asserts on page 5 that it is an inherent property of a cache to update after each occasion of executing. However, in the claimed invention, updating the key is not connected with updating the cache. Regarding dependent Claims 3 and 7, page 5 of the Office Action cites paragraphs [0065]-[0067] of Shirakawa as describing the tamper resistant microprocessor of Claims 3 and 7. However, nowhere does Shirakawa teach or suggest storing the prescribed encryption key stored in the key value register into the secret protection attribute holding section of a cache line for the data, as recited in Claims 3 and 7. Finally, regarding dependent Claims 4 and 8, pages 5-6 of the Office Action cite paragraphs [0081]-[0082] of Shirakawa as describing the tamper resistant microprocessor of Claims 4 and 8. However, nowhere does Shirakawa teach or suggest encrypting a processing result of the data by using the actual encryption key stored in the secret protection attribute holding section of a cache line for the data, as recited in Claims 4 and 8.

Accordingly, it is respectfully submitted that Claims 2-4 and 6-8 are also patentable over Shirakawa because of the features added thereby to their respective independent claim.

Consequently, in view of the present amendment and in light of the above discussions, the outstanding grounds for rejection are believed to have been overcome. The application as amended herewith is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Raymond F. Cardillo, Jr.
Registration No. 40,440

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)